

REDUCTION FROM NON-INJECTIVE HIDDEN SHIFT PROBLEM TO INJECTIVE HIDDEN SHIFT PROBLEM

MIRMOJTABA GHARIBI

*Cheriton School of Computer Science and Institute for Quantum Computing
University of Waterloo, 200 University Avenue West
Waterloo, Ontario N2L 3G1, Canada*

Abstract

We introduce a simple tool that can be used to reduce non-injective instances of the hidden shift problem over arbitrary group to injective instances over the same group. In particular, we show that the average-case non-injective hidden shift problem admit this reduction. We show similar results for (non-injective) hidden shift problem for bent functions. We generalize the notion of influence and show how it relates to applicability of this tool for doing reductions. In particular, these results can be used to simplify the main results by Gavinsky, Roetteler, and Roland about the hidden shift problem for the Boolean-valued functions and bent functions, and also to generalize their results to non-Boolean domains (thereby answering an open question that they pose).

Keywords: quantum computing, efficient algorithm, hidden shift problem, Boolean hidden shift problem, bent functions

1 Introduction

After Shor's discovery of an efficient quantum algorithm for factoring and the discrete log problems, research on the hidden subgroup problem (HSP) attracted many scholars in the field [2]. HSP is a framework which includes factoring and the discrete log in itself [3]. Despite the early success in finding a solution for the abelian HSP, achieving a similar result has proven to be hard for the non-abelian case [3]. HSP is important since solutions for it over the dihedral group and the symmetric group will yield solutions to some lattice problems and graph isomorphism respectively [4, 5, 6, 7]. In both cases, we have a non-abelian instance of HSP.

The hidden shift problem (also known as the hidden translation problem) was defined in the works of [8, 9]. Interesting problems can be stated as a hidden shift problem, most notably this includes hidden subgroup problem over dihedral group, which is equivalent to the hidden shift problem over \mathbb{Z}_N , and graph isomorphism, which can be cast as a hidden shift problem over S_n [10, 11, 12]. The study of the hidden shift problem can give an arguably more natural view to tackle the graph isomorphism problem [12].

In the injective hidden shift problem, we are given two injective functions over some group G that are simply a shifted version of each other. The task is to output such a

shift. More formally, let $f, g : G \rightarrow S$ be two injective functions such that, for some unique $s \in G$, it holds that

$$f(x) = g(sx) \text{ for all } x \in G. \quad (1)$$

The goal is to find the hidden shift s .

Relaxing the requirement for the functions to be injective, will lead to a variant of the problem. We call this new problem, the non-injective hidden shift problem. We restrict the problem to the instances with non-periodic functions, so that the hidden shift will be unique.

By lower bounds on the query complexity of the unstructured search problem, a worst case solution to the non-injective hidden shift problem cannot be obtained [17]. Imposing restrictions on the instances makes the non-injective hidden shift problem more tractable. In particular, in this paper, we are concerned with the average case non-injective hidden shift problem and also the hidden shift problem for bent functions.

The non-injective hidden shift problem has been studied for a variety of functions. Efficient quantum algorithm for solving the hidden shift problem when $f : \mathbb{Z}_p \rightarrow \{-1, 0, 1\}$ is the Legendre symbol is presented in the work by van Dam *et al.* [8]. They also gave a reduction to the injective case based on a conjecture in [7] that any string formed by l subsequent values of f is unique where $l > 2 \log^2 p$. Gavinsky *et al.* gave an efficient quantum algorithm in [1] for solving the hidden shift problem for the average case Boolean functions $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$. Ozols *et al* gave another quantum algorithm for the Boolean hidden shift problem based on a quantum analogue of the rejection sampling defined in their paper [13]. Roetteler gave an efficient quantum algorithm in [14] for solving the hidden shift problem for several classes of the so-called bent functions. Later in [1], the hidden shift problem for all bent functions was solved as a special case of their algorithm. Bent functions are the Boolean functions $f(x) : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ for which applying Hadamard transform to the function $f'(x) := (-1)^{f(x)}$ will yield Fourier coefficients of equal absolute value [15]. A complete characterization of bent functions seems to be a subtle task. However, it can be shown that bent functions do not exist for values of n that are odd [15]. For large enough values of n that are even, bent functions are guaranteed to exist and their count is at least $\Omega\left(2^{2^{n-1} + 1/2 \binom{n}{n/2}}\right)$ [16].

1.1 Our results

In the next section, we introduce a framework that we call *injectivization*. We show that this tool can be used particularly for reducing the average case non-injective hidden shift problem for functions from any abelian or non-abelian group G to any finite set to the injective hidden shift problem over the same group. Also, it can be used to reduce the (non-injective) hidden shift problem for bent functions to the injective hidden shift problem over the same group (which is \mathbb{Z}_2^n). We relate the applicability of this tool to a generalized notion of influence of the function.

These results about the hidden shift problem for the average case Boolean functions and bent functions and the relation to the function's influence simplify the main result in [1]. We show that the Boolean hidden shift problem and the hidden shift problem for bent functions both reduce to Simon's problem since the injective hidden shift problem over \mathbb{Z}_2^n admits a straightforward reduction to Simon's problem. Furthermore, these results answer an open question they ask, whether their methods can be generalized and adapted for the case of non-Boolean functions, as well. We do not use the methods in [1], but using our own method, we generalize the results in [1] to functions whose range are arbitrary sets and are defined over groups of form \mathbb{Z}_q^n with q a constant prime power.

2 Injectivization

Injectivization is a process making it possible to transform two given non-injective functions defined over an arbitrary finite group into two injective functions defined over the same group while preserving the shift structure between them. The framework that we describe below is a way of constructing an injectivization process.

In this paper, we use G to refer to an arbitrary finite group and S to refer to an arbitrary finite set. We denote the k -th component of an m -tuple $V \in G^m$ with v_k .

The injectivization's input and output are specified in the following way:

- Input: any function $f : G \rightarrow S$ and an m -tuple $V \in G^m$,
- Output: function $f_V : G \rightarrow S^m$ constructed in the following way:

$$f_V(x) := (f(xv_1), f(xv_2), \dots, f(xv_m)). \quad (2)$$

We say injectivization succeeds if f_V is injective; otherwise it fails.

2.1 The average case non-injective hidden shift problem

To show that injectivization fails only with small probability when the input function $f : G \rightarrow S$ is chosen uniformly at random, in Theorem 1 we show that the probability of a collision (i.e., the existence of $x, y \in G$ such that $f_V(x) = f_V(y)$) is small if V has distinct components. Note that random variables $f_V(x)$ and $f_V(y)$ are not necessarily independent. We slightly abuse the definition of the non-injective hidden shift problem in Theorem 1 and Corollary 2. We make no promise that functions are not periodic.

Theorem 1: For arbitrary $V \in G^m$ with distinct components and for uniformly random function $f : G \rightarrow S$ the probability that f_V is not injective is at most $\frac{|G|^2}{|S|^{\lceil m/2 \rceil}}$.

Proof: We will show that, for any distinct x and y in the domain, $\Pr[f_V(x) = f_V(y)] \leq 1/|S|^{\lceil m/2 \rceil}$ and then the result follows from the union bound.

Let x and y be any two points in the domain of the function. If all of the components of $(xv_1, xv_2, \dots, xv_m)$ and $(yv_1, yv_2, \dots, yv_m)$ are distinct then it is clear that equality in each component is independent, so $\Pr[f_V(x) = f_V(y)] = 1/|S|^m$. However, the components need not all be distinct in which case there can be dependencies among components. To illustrate, consider the case where $G = \mathbb{Z}_2^n$, $|S| = 2$ and $m = 2$. We use additive notation temporarily. If $x = v_1$ and $y = v_2$ then $(x + v_1, x + v_2) = (0, v_1 \oplus v_2)$ and $(y + v_1, y + v_2) = (v_2 \oplus v_1, 0)$, so a collision in the first component implies a collision in the second component. Therefore, the probability of the collision $f_V(x) = f_V(y)$ is $1/2$ rather than $1/4$.

To address the general case, consider a maximal chain of dependencies:

$$\begin{aligned} xv_{j_1} &= yv_{j_2} \\ xv_{j_2} &= yv_{j_3} \\ &\vdots \\ xv_{j_r} &= yv_{j_{r+1}}. \end{aligned} \quad (3)$$

If $j_{r+1} = j_1$ then we have an r -cycle (the above example is a 2-cycle)(Fig. 1.). Collisions in components j_2, \dots, j_r of $f_V(x)$ and $f_V(y)$ occur independently; however if all these components collide, a collision in the component j_1 is implied (Fig. 2.). Therefore, the probability of a collision among components j_1, \dots, j_r is $1/|S|^{r-1}$. If, on the other hand,

the chain is not cyclic then the probability of a collision among components j_1, \dots, j_{r+1} is $1/|S|^{r+1}$. Since all maximal chains of dependencies are disjoint, the probability of $f_V(x) = f_V(y)$ is the highest when there are $m/2$ 2-cycles, when it is $1/|S|^{\lceil m/2 \rceil}$ (Fig. 3.) ■.

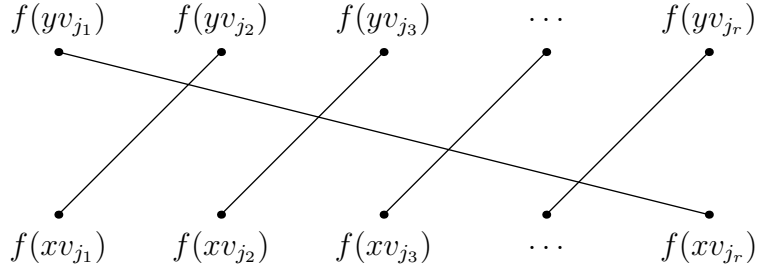


Figure 1: Components are shown with vertices and equal components are connected with an edge.

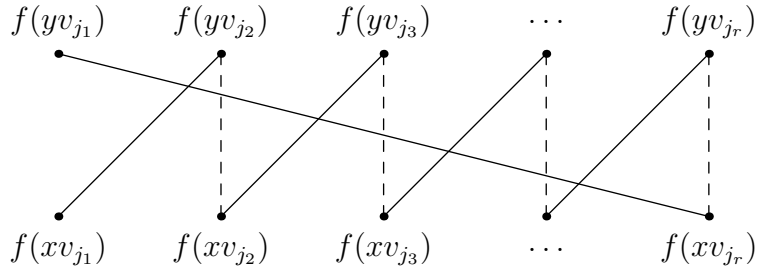


Figure 2: Components are shown with vertices and equal components are connected with an edge. Dashed lines show the collisions.

It is not hard to show that injectivization preserves the shift. More formally, pick an arbitrary $V \in G^m$ where m is any positive integer. Pick functions $f, g : G \rightarrow S$. For any $s \in G$, it holds that $f(x) = g(sx)$ for all $x \in G$ if and only if $f_V(x) = g_V(sx)$ for all $x \in G$. Furthermore, given oracles for f, g , it is straightforward to simulate a query to f_V and g_V efficiently, in both quantum and classical regime. Using these and Theorem 1, we obtain the following corollary.

Corollary 2: Injectivization, when it succeeds, reduces an instance of the non-injective hidden shift problem $f, g : G \rightarrow S$ to an instance of the hidden shift problem $f_V, g_V : G \rightarrow S^m$ where m is the number of V 's components. Injectivization fails with probability at most $\frac{|G|^2}{|S|^{\lceil m/2 \rceil}}$ over the uniform random choice of f .

Theorem 1 specifies an upper bound on the failure rate of the injectivization process when the function f is chosen uniformly at random. Injectivization process always fails when the input function is periodic since the output function also will be periodic. As a

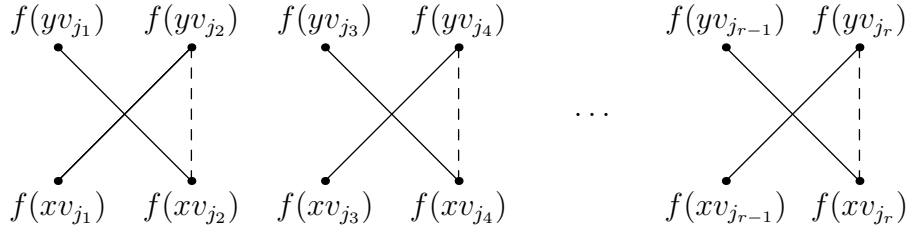


Figure 3: Components are shown with vertices and equal components are connected with an edge. Dashed lines show the collisions.

result, the failure rate when f is a uniformly and randomly chosen function in Corollary 2 is also an upper bound on the failure rate when f is a non-periodic uniformly and randomly chosen function. Using this and Corollary 2, the following corollary is trivial for polynomially large m :

Corollary 3: Let $V \in G^m$ be composed of m distinct components. Having $m \geq (4 + \epsilon) \log_{|S|} |G|$ with an arbitrary constant $\epsilon > 0$, an instance of the non-injective hidden shift problem $f, g : G \rightarrow S$ is reduced to an instance of the hidden shift problem $f_V, g_V : G \rightarrow S^m$ with extremely high probability (asymptotically) over the uniform random choice of the non-periodic function f .

Theorem 2 in [1] states that by the algorithms in [1], an average case exponential separation can be achieved. This result can be simplified by reducing the Boolean hidden shift problem to Simon's problem [18]:

Corollary 4: The average case Boolean hidden shift problem reduces to Simon's problem using injectivization over $f, g : \mathbb{Z}_2^n \rightarrow \{0, 1\}$ and then constructing the blackbox in Simon's problem $h : \mathbb{Z}_2^{n+1} \rightarrow \{0, 1\}^m$ in the following way:

$$h(x_n x_{n-1} \dots x_1 x_0) = \begin{cases} f_V(x_{n-1} x_{n-2} \dots x_0), & \text{if } x_n = 0 \\ g_V(x_{n-1} x_{n-2} \dots x_0), & \text{if } x_n = 1. \end{cases} \quad (4)$$

Gavinsky *et al.* posed an open question in [1] whether the methods they have used for solving the hidden shift over \mathbb{Z}_2^n for the Boolean functions can be generalized and adapted for the case of non-Boolean functions. We have not used the method in [1], but we can say that using injectivization, as described above, we can reduce the average case non-injective hidden shift problem over \mathbb{Z}_2^n to Simon's problem. Since in Simon's problem, it is not important for the functions to have range in binary strings, our functions need not be binary and they can have range in any finite set S . Furthermore, considering the domain to be the group \mathbb{Z}_q^n with $q \geq 3$ a constant prime power, using injectivization, we can reduce the problem to the already solved injective case [9, 19].

2.2 Relation between the hidden shift problem and influence over the functions

We extend the notion of influence to the functions defined over any group G and having range in any set S . The influence of v over $f : G \rightarrow S$ is defined as $\gamma_v(f) = \Pr_x[f(x) \neq$

$f(xv)$. When $G = \mathbb{Z}_2^n$ and $S = \{0, 1\}$, this definition reduces to the conventional notion of influence. It is not hard to see that the function f is periodic if and only if for some $v \in G \setminus \{1\}$: $\gamma_v = 0$. Thus, the hidden shift problem with underlying functions f, g is well-defined if the minimum influence of f , that is, $\gamma_{\min}(f) := \min_{v \in G \setminus \{1\}}(\gamma_v(f))$ is not zero.

Theorem 5: For a uniformly at random chosen $V \in G^m$ and a function $f : G \rightarrow S$ the probability that f_V is not injective is at most $\frac{N}{2} \sum_{x \in G} (1 - \gamma_x)^m \leq N^2(1 - \gamma_{\min})^m$.

Proof: Let N denote $|G|$. We define the matrix $A_{N \times N}$ according to

$$A_{N \times N} = \begin{bmatrix} f(x_0x_0) & f(x_1x_0) & \dots & f(x_{N-2}x_0) & f(x_{N-1}x_0) \\ f(x_0x_1) & f(x_1x_1) & \dots & f(x_{N-2}x_1) & f(x_{N-1}x_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ f(x_0x_{N-2}) & f(x_1x_{N-2}) & \dots & f(x_{N-2}x_{N-2}) & f(x_{N-1}x_{N-2}) \\ f(x_0x_{N-1}) & f(x_1x_{N-1}) & \dots & f(x_{N-2}x_{N-1}) & f(x_{N-1}x_{N-1}) \end{bmatrix} \quad (5)$$

where $x_0, x_1, x_2, \dots, x_{N-1}$ is an enumeration of elements of G in an arbitrary order.

For any two fixed and distinct rows i, j , the probability that their k -th element are equal is exactly $1 - \gamma_{(x_i^{-1}x_j)}$ when k is chosen uniformly at random. Thus, the probability that the strings of m randomly chosen elements are equal is $(1 - \gamma_{(x_i^{-1}x_j)})^m$ since the events are independent. Using union bound, it can be seen that the probability that any two strings of the form above are equal for any two distinct rows is at most

$$\begin{aligned} \sum_{i < j} (1 - \gamma_{(x_i^{-1}x_j)})^m &= \frac{N}{2} \sum_{x \in G \setminus \{1\}} (1 - \gamma_x)^m = \frac{N}{2} \sum_{x \in G} (1 - \gamma_x)^m \\ &\leq N^2(1 - \gamma_{\min})^m. \end{aligned}$$

Based on the construction, this is an upper bound on the probability that f_V is a non-injective function ■.

In [1], the number of queries needed by their algorithm to solve the hidden shift problem for functions of form $f, g : \mathbb{Z}_2^n \rightarrow \{0, 1\}$ is shown to be related to the minimum influence of f . Interestingly, Theorem 5 relates the success probability of injectivization to the same intrinsic feature of the function, that is, the minimum influence. To be precise, we are using the generalized notion of influence, but it remains the same for the case of binary functions. Hence, this gives an alternative proof that the average case Boolean functions can be injectivized when V is chosen uniformly at random, due to a lower bound on the minimum influence of the majority of the Boolean functions in [1]. As a special case of this, using injectivization, it is possible to efficiently reduce the hidden shift problem for bent functions to the Simon's problem. Bent functions have a property called perfect nonlinearity, which means that, for any bent function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ and for any non-zero $v \in \mathbb{Z}_2^n$, the function $f_v(x) := f(x) + f(x + v)$ is a balanced Boolean function [20]. This is equivalent to saying that $\gamma_v(f) = \gamma_{\min}(f) = 1/2$ for any non-zero v . Using Theorem 5 and a construction similar to Corollary 4, we have the following corollary:

Corollary 6: Choosing $m > (2 + \epsilon)n$ with an arbitrary constant $\epsilon > 0$, using injectivization, the hidden shift problem for bent functions $f, g : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ reduces to the injective hidden shift problem $f_V, g_V : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ with high probability (asymptotically) which in turn reduces to Simon's problem.

3 Classical complexity

We show that, the classical query complexity of the non-injective hidden shift problem when the underlying group is \mathbb{Z}_m^n is high in the average case when m is a constant number. For proving this bound, we benefit from some of the ideas in [1].

First, we define an artificial variant of the non-injective hidden shift problem which helps in proving the classical lower bound on the complexity of the average case non-injective hidden shift problem. We call this problem, the no-promise non-injective hidden shift problem. The only difference in this new problem is that we first pick $s \in G$ and oracle $g : G \rightarrow S$. Then the oracle $f : G \rightarrow S$ will be constructed according to (1). The goal of the problem is to find s given oracles f and g . In this problem, when f and g happen to be periodic functions, information theoretically it is not possible to choose the right s with certainty among the many possible candidates.

Similar to [1], queries are made to the pair of functions (f, g) . This at most doubles the number of queries which is not important in the context of query complexity.

Theorem 7: To solve a uniformly random instance of the no-promise non-injective hidden shift problem defined with a solution $s \in \mathbb{Z}_q^n$ and functions $f, g : \mathbb{Z}_q^n \rightarrow S$ with probability at least $1/2$, at least $\Omega\left(p_1^{n/2}\right)$ queries are needed when q is a constant number and p_1 is the smallest prime divisor of q .

Proof: Let $q = p_1^{k_1} \times p_2^{k_2} \cdots \times p_t^{k_t}$ be the prime factorization of q where $p_1 < p_2 < \cdots < p_t$ holds. Let T_1, T_2, \dots, T_m be an enumeration of all 1-dimensional subspaces of $\mathbb{Z}_{p_1}^n$. Since p_1 is a prime number, all subspaces have the same number of elements. Furthermore, the only common element between each two subspaces is 0. These two imply $m = \frac{p_1^n - 1}{p_1 - 1}$.

We define the disjoint sets $S_i = T_i \setminus \{0\}$ for all $1 \leq i \leq m$. We use the following notation: for $x \in \mathbb{Z}_q^n$, we define $x_{p_1} \in \mathbb{Z}_{p_1}^n$ such that $x_{p_1} = (x \bmod p_1)$ where $\bmod p_1$ is carried out component-wise.

As a bonus to the classical computer, we provide a magical bell to it which rings if it makes the queries X_1 and X_2 and it happens that $(X_1 - X_2)_{p_1}$ and s_{p_1} are both in the same set S_i . If finding in which set s_{p_1} lies, proves to be hard, then finding s itself must be hard because of an obvious reduction from the latter to the former.

Without loss of generality, we assume $s_{p_1} \neq 0$. Let $Q_k = \{X_1, X_2, \dots, X_k\}$ be the places in which the queries are made after k queries. Also, let D be the set of all i 's for which we know $s_{p_1} \notin S_i$ according to our queries and the magical bell. The sets S_1, S_2, \dots, S_m are disjoint. This gives the important observation that knowing D gives no information about the actual set to which s_{p_1} belongs. More formally, we have

$$\Pr[s_{p_1} \in S_i | i \notin D] = \frac{1}{m - |D|} \leq \frac{1}{\frac{p_1^n - 1}{p_1 - 1} - k^2}. \quad (6)$$

Since conditioning on the queries does not provide any information, the best algorithm is to just randomly guess the set to which s_{p_1} belongs. The best a classical computer can do is to eliminate $1 + \binom{k}{2} \leq k^2$ possible sets after k queries. Hence, to be able to find the set to which s_{p_1} belongs with probability at least $1/2$, it needs to make at least $\Omega\left(p_1^{n/2}\right)$ queries ■.

Theorem 8: To solve the non-injective hidden shift problem for functions $f, g : \mathbb{Z}_q^n \rightarrow S$ with probability at least $1/2 + \epsilon$ classically, $\Omega\left(p_1^{n/2}\right)$ queries are needed in the average

case, when $\epsilon > 0$ is an arbitrary constant.

Proof: The probability that f is periodic is very small. More formally, for any fixed non-zero $r \in \mathbb{Z}_q^n$, it holds that

$$\Pr[f(x+r) = f(x) \text{ for all } x] \leq \frac{1}{|S|^{q^n/2}} \quad (7)$$

where the probability of the event is the highest when the order of r is 2. Hence, by the union bound, the probability of having a periodic function is at most $\frac{q^n}{|S|^{q^n/2}}$ which is double exponentially small. This implies that the number of periodic functions is at most $R := N \frac{q^n}{|S|^{q^n/2}}$ where $N := |S|^{q^n}$ denotes the total number of functions.

As the name suggests, adding the promise that the functions are non-periodic makes the no-promise non-injective hidden shift problem the same as the injective hidden shift problem in definition. Since the number of periodic functions is negligible, the uniform probability distribution over the whole language, U , is extremely close in variation distance to the uniform probability distribution over non-periodic functions, V . More formally:

$$\|U - V\| = \frac{1}{2} \sum_{x \in L} |U(x) - V(x)| \leq \frac{1}{2} \left((N - R) \left(\frac{1}{N - R} - \frac{1}{N} \right) + \frac{R}{N} \right) = \frac{R}{N}. \quad (8)$$

Using Theorem 7, it implies immediately that there should not exist a probabilistic classical Turing machine that makes less than $\Omega(p_1^{n/2})$ queries and solves a uniformly random chosen instance of the non-injective hidden shift problem with probability at least $\frac{1}{2} + \frac{R}{N}$, otherwise we could use this Turing machine to violate Theorem 7 ■.

4 Conclusion

We developed a framework called injectivization which can be used for reducing some instances of the non-injective hidden shift problem over any group to the hidden shift problem for injective functions over the same group. In particular, we showed that this process succeeds, when we have an average case instance of the non-injective hidden shift problem and also when the underlying function is bent. We related the success probability of this process to a generalized notion of influence. In addition, we simplified the main result of [1] and also used this framework to address an open question of [1] by generalizing their results to the hidden shift problem for functions $f, g : \mathbb{Z}_q^n \rightarrow S$ where S is an arbitrary set and q is a constant prime power. We also proved that the average case classical complexity of this problem for any constant q is high.

Acknowledgements

We are grateful to Richard Cleve for helpful discussions and his revision of this paper and to Andrew Childs for fruitful discussions. We also thank Dmitry Gavinsky for helpful email correspondence and the anonymous referee for the comments that significantly improved this work.

References

- [1] D. Gavinsky, M. Roetteler, J. Roland (2011), *Quantum algorithm for the Boolean hidden shift problem*, In Proceedings of the 17th annual international conference on Computing and Combinatorics, COCOON '11, pp. 158-167, Berlin, Heidelberg.
- [2] P. Shor (1997), *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput., 26, pp. 1484-1509.
- [3] A. Childs and W. van Dam (2010), *Quantum algorithms for algebraic problems*, Rev. Mod. Phys., 82, pp 1-52.
- [4] R. Beals (1997), *Quantum computation of Fourier transforms over symmetric groups*, In Proceedings of the twenty-ninth annual ACM symposium on Theory of Computing, STOC '97, pp 48-53, New York, NY, USA.
- [5] M. Ettinger and P. Høyer (1999), *A Quantum Observable for the Graph Isomorphism Problem*, quant-ph/9901029.
- [6] P. Høyer (1997), *Efficient Quantum Transforms*, quant-ph/9702028.
- [7] D. Boneh and R. Lipton (1995), *Quantum cryptanalysis of hidden linear functions (extended abstract)*, In Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '95, pp. 424-437, London, UK.
- [8] W. van Dam, S. Hallgren, and L. Ip (2003), *Quantum algorithms for some hidden shift problems*, In Proceedings of the fourteenth annual ACM-SIAM Symposium on Discrete Algorithms, SODA '03, pp. 489-498, Philadelphia, PA, USA.
- [9] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen (2003), *Hidden translation and orbit coset in quantum computing*, Proceedings of the 35th ACM Symposium on Theory of Computing, pp. 1-9.
- [10] M. Ettinger and P. Høyer (2000), *On quantum algorithms for noncommutative hidden subgroups*, Advances in Applied Mathematics, 25, pp. 239-251.
- [11] G. Kuperberg (2005), *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM Journal on Computing 35(1), pp. 170-188.
- [12] A. Childs and P. Wocjan (2007), *On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems*, Quantum Info. Comput., Vol.7, pp. 504-521.
- [13] M. Ozols, M. Roetteler, and J. Roland (2011), *Quantum rejection sampling*, arXiv:1103.2774v4 [quant-ph].
- [14] M. Roetteler (2010), *Quantum algorithms for highly non-linear Boolean functions*, In Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '10, pp. 448-457, Philadelphia, PA, USA.
- [15] O. Rothaus (1976), *On "bent" functions*, J. Comb. Theory, Ser. A, pp. 300-305.
- [16] C. Carlet and P. Gaborit (2006), *Hyper-bent functions and cyclic codes*, Journal of Combinatorial Theory, Series A, 113(3), pp. 466-482.
- [17] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani (1997), *Strengths and weaknesses of quantum computing*, SIAM J. Comput., 26, pp. 1510-1523.
- [18] D. Simon (1997), *On the power of quantum computation*, SIAM Journal on Computing, 26, pp. 116-123.
- [19] G. Ivanyos (2008), *On solving systems of random linear disequations*, Quantum Info. Comput., Vol.8, pp. 579-594.
- [20] W. Meier and O. Staffelbach (1990), *Nonlinearity Criteria for Cryptographic Functions*, Advances in Cryptology - EUROCRYPT 89, vol.434, pp. 549-562, Berlin, Heidelberg